CLAIMS:

What is claimed is:

1. A computer network, comprising:

a client and a server connected by a network connection, wherein the client has a userid and a password associated with the client;

wherein the client requests access to the server by sending a first set of values to the server;

wherein the server responds to the client by generating a one-time challenge token that depends at least on a first random value and sending the challenge token to the client;

wherein the client retrieves the first random value from the challenge token and sends the first random value and the userid to the server;

wherein the server verifies the received first random value from the client is correct, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server.

2. The computer network of claim 1, wherein the first set of values including a first random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one.

3. The computer network of claim 1, wherein the client verifies the validity of the one-time authentication token.

4. The computer network of claim 1, wherein the server generates the challenge token by exclusive-oring the first random value with a first hash.

5. The computer network of claim 4, wherein the first hash is a hash of the following:

a primitive root of a large prime number raised to a power, a digest of the client's userid and password, and a second random value.

6. The computer network of claim 1, wherein the server verifies the received first random value from the client is correct by comparing the first random value received from the client with the server's stored value of the first random number.

7. The computer network of claim 1, wherein the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the result, the userid, and the message authentication code to the server;

wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code, and wherein if the received message authentication code is verified, the server changes the client password.

8. The computer network of claim 7, wherein the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password.

9. A computer program product in a computer readable medium, comprising:

a client and a server connected by a network connection, wherein the client has a userid and a password associated with the client;

first instructions whereby the client requests access to the server by sending a first set of values to the server;

second instructions whereby the server responds to the client by generating a one-time challenge token that depends at least on a first random value and sending the challenge token to the client;

third instructions whereby the client retrieves the first random value from the challenge token and sends the first random value and the userid to the server;

fourth instructions whereby the server verifies the received first random value from the client is correct, and if so, the server generates a one-time authentication token and sends it to the client, giving it permission to access the server.

10. The computer program product of claim 9, wherein the first set of values including a first random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one.

11. The computer program product of claim 9, wherein the client verifies the validity of the one-time authentication token.

12. The computer program product of claim 9, wherein the server generates the challenge token by exclusive-oring the first random value with a first hash.

13. The computer program product of claim 12, wherein the first hash is a hash of the following:

a primitive root of a large prime number raised to a power, a digest of the client's userid and a password, and a second random value.

14. The computer program product of claim 9, wherein the server verifies the received first random value from the client is correct by comparing the first random value received from the client with the server's stored value of the first random number.

15. The computer program product of claim 9, wherein the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to form a result, and sending the result, the userid, and the message authentication code to the server;

wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code, and wherein if the received message authentication code is verified, the server changes the client password.

16. The computer program product of claim 15, wherein the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password.

17. A method of authenticating a client with a server across a network connection, comprising the steps of:

requesting, by the client, access to the server by sending a first set of values to the server;

responding, by the server, to the client by generating a one-time challenge token that depends on at least a first random value and sending the challenge token to the client;

retrieving, by the client, the first random value from the challenge token;

sending, by the client, the first random value and a userid of the client to the server;

verifying, by the server, the received first random value from the client;

if the first random value from the client is verified by the server, generating a one-time authentication token by the server;

sending the one-time authentication token to the client to thereby give the client permission to access the server.

18. The method of claim 17, wherein the first set of values including a first random value, a large prime number, a primitive root of the large prime number, and a large random integer less than the large prime number minus one.

19. The method of claim 17, wherein the client verifies the validity of the one-time authentication token.

20. The method of claim 17, wherein the server generates the challenge token by exclusive-oring the first random value with a first hash.

21. The method of claim 20, wherein the first hash is a hash of the following:

a primitive root of a large prime number raised to a power, a digest of the client's userid and a password, and a second random value.

22. The method of claim 17, wherein the server verifies the received first random value from the client is correct by comparing the first random value received from the client with the server's stored value of the first random number.

23. The method of claim 17, wherein the client changes the password by computing a hash of the userid and a new password to form a new digest, creating a mask, computing a message authentication code, and by exclusive-oring the mask with the new digest to

form a result, and sending the result, the userid, and the message authentication code to the server;

wherein the server retrieves the new digest by exclusive-oring the mask with the received result, and wherein the server verifies the received message authentication code, and wherein if the received message authentication code is verified, the server changes the client password.

24. The method of claim 23, wherein the server changes the client password by replacing a digest of at least the old password with a digest of at least the new password.